ITU KALEIDOSCOPE
ATLANTA 2019

Thought-Based Authenticated Key Exchange

Phillip H. Griffin
Griffin Information Security
phil@phillipgriffin.com

4-6 December
Atlanta, Georgia, USA

Identity Authentication Factors

- **Something You Know** – A “weak secret”, such as a password or PIN
- **Something You Are** – A biometric sample, such as voice, face, or iris
- **Something You Have** – A card, token, proof of private key possession

*User account names are **public**.*

*Identity authentication factors are **secrets** that must be protected*.

Multiple authentication factors provide stronger identity assurance.

Password Authenticated Key Exchange

PAKE - Standardized in **ITU-T Rec. X.1035** and in ISO/IEC 11770-4

User establishes an ***Account*** and a ***Password*** on a server

To login, ***Password*** is used to create a ***Key*** that encrypts a server challenge

The encrypted challenge is sent to the server with an unencrypted ***Account***

Server receives encrypted challenge and **Account** locates user ***Passwor***d

Server ***Password*** creates ***Key,*** decrypts challenge to authenticate user

Server encrypts a response to challenge for user to mutually authenticate

X.1035 can be extended to support multi-factor user authentication, by adding biometric and possession factors to the encrypted server challenge

What about people who can’t use passwords?

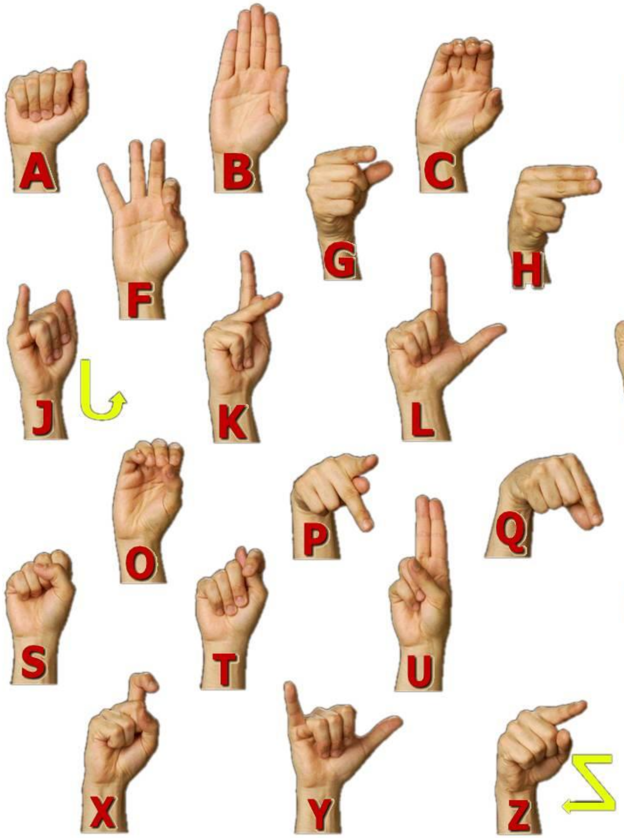
Passwords are needed to operate PAKE, but they can come from many sources:

- Traditionally, passwords come from keyboard, keypad, or touch screen entry
- Biometric sensors can sometimes collect two authentication factors at once
- Model-based sensor devices can map their results to password strings

An obvious example of passwords from biometric sensors is recorded voice data

Speech Recognition can extract a password from voice data
Speaker Recognition can use voice data for biometric matching

Something-You-Know & Something-You-Are



Modeled sensor data mapped to passwords

Hand Sign	Password Substitution String
	R'W]$Pq57]mbTkG7j+$Uqe3#kbCf
	$ZkQB[ax<)p4D#QsWK}um<~k3D%
	K9hWFDeLG8,“O)hLNSaCF#<`A!U2
	eX2:]C97”P^~;Swhl={H04<"%A;U

ITU-T Standardization Opportunities

Extend ITU-T Rec. X.1035 Password Authenticated Key (PAK) Exchange

Define an OID to identify each unique mechanism (as in ISO/IEC 11770-4)

Specify processing for multifactor user authentication

Define an X.894 payload for information exchange between the user & server

Extend X.tas: Telebiometric authentication using speaker recognition

Support face and hand biometrics from camera collected sensors

Extend ITU-T Rec. X.1080.0 Access Controls to support X.1035 PAKE

PAKE can provide a low cost, certificateless alternative to CMS and TLS

Create a new PAKE-extended TLS standard for certificateless mobile users

Support multifactor TLS user authentication & low cost mutual authentication

Revise ITU-T Rec. X.1081 framework to include non-telebiometric devices

Consider EEG data and other “human body meets electronic” devices

ITU KALEIDOSCOPE
ATLANTA 2019

Thank you